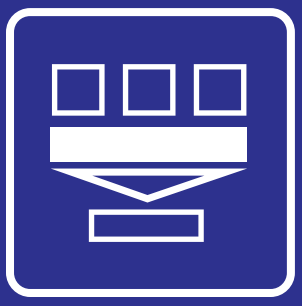


FORTINET

FortiOS™ Handbook - Virtual Domains

VERSION 6.0.2

FORTIOS VERSION 6.0

FORTINET DOCUMENT LIBRARY

https://docs.fortinet.com

FORTINET VIDEO GUIDE

https://video.fortinet.com

FORTINET KNOWLEDGE BASE

http://kb.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTINET COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING AND CERTIFICATION PROGRAM

https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE

https://training.fortinet.com/

FORTIGUARD CENTER

https://fortiguard.com

FORTICAST

http://forticast.fortinet.com

END USER LICENSE AGREEMENT

https://www.fortinet.com/doc/legal/EULA.pdf

August 21, 2018

FortiOS™ Handbook - Virtual Domains

01-602-481102-20180821

TABLE OF CONTENTS

Change log **5**
Introduction **6**
What's new in FortiOS 6.0 6
VDOMs overview **7**
Benefits of VDOMs 7
Savings in physical space and power 7
Combining NAT mode and transparent mode 7
MSSP configuration 8
Virtual clustering 8
VDOM configurations 8
Independent VDOMs 8
Management VDOM 9
Meshed VDOMs 9
Configuring VDOMs **11**
Enabling VDOMs on your FortiGate 11
The root VDOM 11
Enabling virtual domains 11
Global and per-VDOM settings 12
Changes to the GUI and CLI 12
Resource settings 12
Increasing the maximum number of VDOMs 14
Configuring additional VDOMs 14
Creating a VDOM 15
Changing the management VDOM 16
Assigning interfaces to a VDOM 16
Per-VDOM administrators 17
Certificate management 18
Security profiles 18
Disabling a VDOM 19
Deleting a VDOM 20
Inter-VDOM routing 20
Types of inter-VDOM links 21
HA virtual clusters 21
Creating inter-VDOM links 22

Deleting VDOM links 23
VDOMs in NAT mode 24
Using a VDOM in NAT/route mode 24
Configuring VDOM routing 24
Configuring security policies 26
Changing the inspection mode 27
Configuring VPNs for a VDOM 27
Example configuration: VDOM in NAT/route mode 28
Network topology and assumptions 28
General configuration steps 29
Creating the VDOMs 29
Configuring the FortiGate interfaces 30
Configuring the vdomA VDOM 32
Configuring the vdomB VDOM 35
Testing the configuration 37
VDOMs in transparent mode 39
VDOMs in transparent mode 39
Using a VDOM in transparent mode 39
Switching to transparent mode 40
Adding VLAN subinterfaces 40
Creating security policies 40
Example configuration: VDOM in transparent mode 41
Network topology and assumptions 42
Configuring common items 42
Creating virtual domains 43
Configuring the Company_A VDOM 43
Configuring the Company_B VDOM 47
Configuring the VLAN switch and router 52
Testing the configuration 53
Troubleshooting VDOMs 55
The option to enable VDOMs is missing 55
Administrators can't access their assigned VDOM 55
Your FortiGate is running slowly 56
Your license for additional VDOMs doesn't appear 56
You can't delete a VDOM 56
A non-management VDOM isn't working with SNMP 56

Change log

Date	Change description
August 21, 2018	Minor updates throughout.
July 26, 2018	FortiOS 6.0.2 document release. Minor updates.
June 5, 2018	FortiOS 6.0.1 document release. Minor updates.
March 29, 2018	FortiOS 6.0 document release. See "What's new in FortiOS 6.0" on page 6.

Introduction

This guide explains how to set up and use Virtual Domains (VDOMs) with a FortiGate. It contains the following sections:

- VDOMs overview: information about the basic concepts of VDOMs.
- Configuring VDOMs: procedures for enabling and configuring VDOMs, including inter-VDOM routing.
- VDOMs in NAT mode: detailed explanations and examples for configuring VDOM features for a FortiGate in NAT/route mode.
- VDOMs in transparent mode: detailed explanations and examples for configuring VDOM features for a FortiGate in transparent mode.
- Troubleshooting VDOMs: diagnostic and troubleshooting information for some potential VDOM issues.

What's new in FortiOS 6.0

The following list contains new VDOM features added in FortiOS 6.0. Click on a link to navigate to that section for further information.

- Global security profiles

VDOMs overview

You can use virtual domains (VDOMs) to divide a FortiGate into two or more virtual devices that function independently. For each separate VDOM, you can create different configurations, including firewall policies, routing, VPNs, and security profiles.

Once you have created a VDOM, the steps you need to take to configure it are typically the same as if you were configuring a single FortiGate with VDOMs disabled. This chapter focuses on considerations that are unique to a network using VDOMs.

The Fortinet Security Fabric doesn't support FortiGate units with multiple VDOMs.

Benefits of VDOMs

VDOMs provide the following benefits:

- Savings in physical space and power
- Combining NAT mode and transparent mode
- MSSP configuration
- Virtual clustering

Savings in physical space and power

To increase the number of physical FortiGate devices, you require rack space, cables, and power. You also need to change your network configuration to accommodate the new devices. Finally, if you don't need as many devices in the future, you're left with expensive hardware that you aren't using.

Increasing the number of VDOMs requires no additional hardware and minimal changes to existing networking configurations. VDOMs save physical space and power. You're limited only by the size of your VDOM license and the physical resources of your FortiGate. By default, most FortiGate devices support a maximum of ten VDOMs, and many models allow you to buy a license to increase the maximum number of VDOMs.

Each physical FortiGate also requires a separate FortiGuard license to access security updates. VDOMs don't require you to buy separate licenses, as the same license is shared for all VDOMs located on the same FortiGate. When you update or upgrade the license, the changes are immediately available for all VDOMs.

Combining NAT mode and transparent mode

With multiple VDOMs, you can configure one VDOM configured in transparent mode and other VDOMs in NAT mode. In this configuration, you can use the transparent mode VDOM for troubleshooting your network and the NAT mode VDOMs for networking.

MSSP configuration

If you require a managed security service provider (MSSP) configuration, you can use VDOMs to provide a multi-tenant solution, with each tenant's network connected to a unique VDOM that's configured to meet the network requirements. For each VDOM, you can either manage it globally using the management VDOM or allow tenants to manage their own VDOM.

Virtual clustering

Virtual clustering is an extension of FortiGate high availability for a cluster of two FortiGate units with multiple VDOMs. Virtual clustering provides failover protection for a multiple VDOM configuration and can load balance traffic between the VDOMs to improve overall network performance.

Virtual-clustering load balancing efficiently load balances all traffic between VDOMs and can be adjusted in real time to actively optimize load sharing between the cluster units without affecting the operation of VDOMs in the cluster.

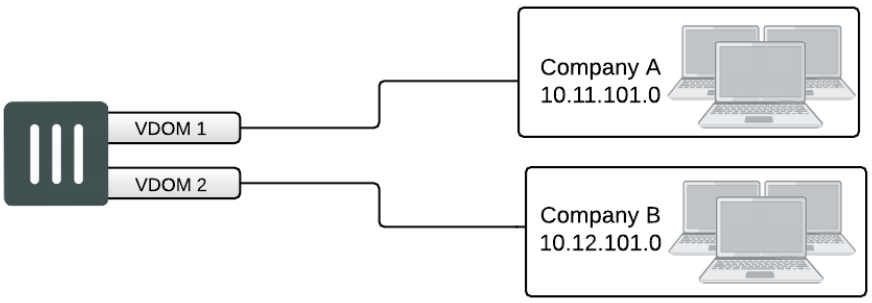
VDOM configurations

There are three main types of VDOM configurations:

- Independent VDOMs
- Management VDOM
- Meshed VDOMs

The main difference between these configurations is whether inter-VDOM routing is used. For more information, see Inter-VDOM routing.

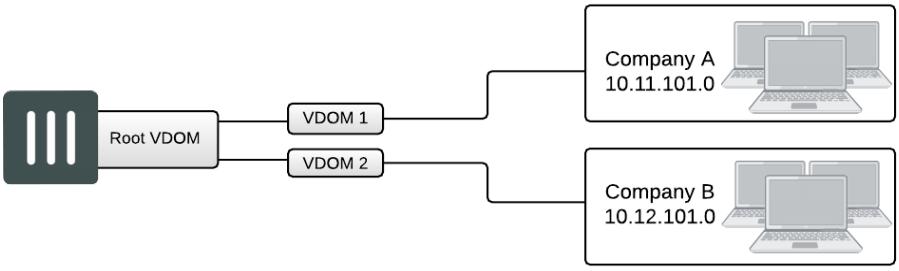
Independent VDOMs



Independent VDOMs is a common configuration. In this configuration, you create multiple VDOMs that are completely separate from each other, without any inter-VDOM routing. Any VDOM in this configuration can be the management VDOM, provided there is Internet access.

This configuration can be used when more than one department or company shares the FortiGate. Using independent VDOMs, each company or department appears to have its own FortiGate, which can be independently managed.

Management VDOM



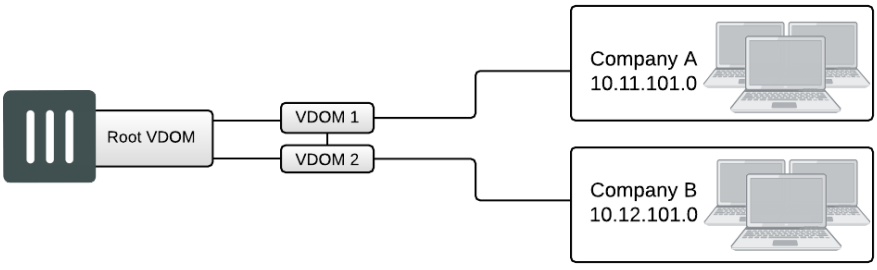
In the management VDOM configuration, the management VDOM is located between the other VDOMs and the Internet. The other VDOMs connect to the management VDOM with inter-VDOM links, with no other inter-VDOM connections.

In this configuration, the management VDOM has full control over access to the Internet, including what types of traffic are allowed in both directions. There is no communication directly between the non-management VDOMs. Security is greatly increased with only one point of entry and exit. Only the management VDOM needs to be fully managed to ensure network security in this case. Each client network can manage its own configuration without compromising security or bringing down another client network.

This configuration can be used for MSSPs, allowing the service provide to administer the management VDOM with the other VDOMs as managed by their customers. The service provider controls the traffic and can prevent the customers from using banned services and prevent Internet connections from initiating those same banned services. Firewall policies control the traffic between the customer VDOM and the management VDOM and can be customized for each customer.

The management VDOM configuration is limited in that the customer VDOMs have no inter-connections. In many situations, this limitation is ideal because it maintains proper security. However, some situations may require customers to communicate with each other, which would be easier if the customer VDOMs were inter-connected.

Meshed VDOMs



The meshed VDOMs configuration, including partial and full mesh, has VDOMs inter-connected using VDOM links. In a partial mesh, only some VDOMs are inter-connected while in a full mesh configuration, all VDOMs are inter-connected.

This configuration can be used when you want to provide full access between VDOMs, but need to handle traffic differently for each VDOM. When you use a meshed VDOM configuration, it is important to ensure proper security. You can achieve this using firewall policies and ensuring secure account access for all administrators and users.

Configuring VDOMs

This section includes the following information about how to configure VDOMs:

- Enabling VDOMs on your FortiGate
- Configuring additional VDOMs
- Inter-VDOM routing

Enabling VDOMs on your FortiGate

This section contains the following topics:

- The root VDOM
- Enabling virtual domains
- Global and per-VDOM settings
- Changes to the GUI and CLI
- Enabling VDOMs on your FortiGate
- Resource settings
- Increasing the maximum number of VDOMs

The root VDOM

On every FortiGate there is a root VDOM that you can't delete. When VDOMs are disabled, the root VDOM isn't visible. When VDOMs are enabled, the root VDOM is visible. The root VDOM is the only VDOM available for configuration, until you enable VDOMs.

Typically, you use the root VDOM as the management VDOM. By connecting to the management VDOM, you can access the global settings for the FortiGate as well as the settings for each individual VDOM. You can set any VDOM to be the management VDOM.

Enabling virtual domains

VDOMs are disabled by default. When you enable VDOMs on your FortiGate, your current configuration is saved, with all parts assigned to the root VDOM. Also, no reboot is required when enabling VDOMs.

To enable VDOMs - GUI:

1. Go to **System > Settings**.
2. Under **Operations Settings**, enable **Virtual Domains**.

The FortiGate logs off all sessions. You can now log in again as admin.

To enable VDOMs - CLI:

```
config system global
   set vdom-admin enable
```

```
end
```

Global and per-VDOM settings

Settings that you configure outside a VDOM are called global settings. These settings affect the entire FortiGate and include areas such as interfaces, DNS, firmware, etc. This also includes some logging and sandboxing options, such as FortiAnalyzer, SNMP, and FortiSandbox. Global settings should only be changed by your top level administrator.

Settings that you configure within a VDOM are called VDOM settings. These settings affect only a specific VDOM and include areas such as operating mode, routing, firewall, VPN, some antivirus, some logging settings, and reporting.

When virtual domains are disabled, the entire FortiGate is effectively a single VDOM, but per-VDOM limits apply. For some resource types, the global limit can't be reached with only one VDOM.

Changes to the GUI and CLI

When you enable VDOMs, the FortiGate GUI and the CLI change, allowing you to manage both global settings and per-VDOM settings. Only admin accounts using the super_admin profile can access global options and settings for all VDOMs. Other administrator accounts can configure only the VDOM they're assigned to.

Other changes only affect either the GUI or the CLI.

GUI:

- When you access the management VDOM (this is the root VDOM by default), you can use the drop-down menu in the top left of the GUI to switch between global and per-VDOM settings. Some menu items only appear under **Global**, while others only appear as per-VDOM settings.
- A menu item is available at **Global > System > VDOM**. You use this to create, edit, and delete VDOMs.
- A menu item is available at **Global > System > Global Resources**. You use this to manage how system resources are shared between VDOMs.

CLI:

- To configure global settings, you must first enter the following CLI to select global options:

  ```
  config global
  ```

- To configure per-VDOM settings, you must first enter the following CLI to select a VDOM:

  ```
  config vdom
    edit <vdom_name>
  ```

Resource settings

Your FortiGate has a limited amount of hardware resources, such as memory, disk storage, and CPU operations. When you use VDOMs, you can control how resources are shared between each VDOM to optimize resource usage. This allows you to ensure the proper level of service is maintained on each VDOM.

For example, if one VDOM is connected to a web server and logging server, and a second VDOM is connected to an internal network of 20 users, these two VDOMs require different levels of resources. The first VDOM requires

many sessions but no user accounts. The second VDOM is the opposite, requiring user accounts and management resources, but fewer sessions.

Global resources

Global resources apply to the entire FortiGate. By default, the values are set to their maximum values. These values vary by FortiGate model because each model has different hardware capabilities. It can be useful to change the maximum values for some resources to ensure there is enough memory available for other resources that might be more important to your configuration.

For example, if your FortiGate is protecting a number of web servers and other publicly accessible servers, you should maximize the available sessions and proxies, and minimize unused settings, such as users or VPNs.

To view the resource list, go to **Global > System > Global Resources**. You can also use the following CLI command:

```
config global
   config system resource-limits
   get
```

Note that some global resources are only be visible if your FortiGate supports those resources. For example, the quota for logging to disk is only visible when your FortiGate has a hard disk.

For explicit proxies, when you configure limits on the number of concurrent users, you need to allow for the number of users based on their authentication method. Otherwise you might run out of user resources.

Each session-based authenticated user is counted as a single user using their authentication membership (RADIUS, LDAP, FSAE, local database, etc.) to match users in other sessions. So one authenticated user in multiple sessions is still one user.

For all other situations, the source IP address is used to determine a user. All sessions from a single source address are assumed to be from the same user.

Per-VDOM resource settings

Each VDOM has its own resource settings, including both maximum and minimum levels. By default, all per-VDOM resource settings are set to allow the maximum. The maximum level is the highest amount of that resource that the VDOM can use if it is available on the FortiGate. Minimum levels are guaranteed levels that are always available, no matter what resources other VDOMs are using.

For example, one VDOM, called VDOM-1, has a maximum of 5000 sessions and a minimum of 1000 sessions. If the FortiGate has a global maximum of 20,000 sessions split among 10 VDOMs, it is possible that VDOM-1 won't be able to reach the 5000 session maximum. However, at all times VDOM-1 is guaranteed to have 1000 sessions available.

To view per-VDOM resource settings - GUI:

1. Select **Global > System > VDOM**.
2. Select the root VDOM, and select **Edit**.
3. Adjust the settings in the **Resource Usage** section of the page.
4. Select **OK**.

To view per-VDOM resource settings - CLI:

```
config global
   config system vdom-property
      edit root
   get
```

Increasing the maximum number of VDOMs

By default, most FortiGate models support a maximum of 10 VDOMs. For certain models, you can purchase a license key to increase the maximum number of VDOMs.

To find out how many VDOMs your FortiGate can support, refer to the data sheet for your model. For more information, see the Fortinet Data Sheets.

It is important to back up your configuration before upgrading the VDOM license on your FortiGate, especially if you're using HA mode.

To obtain a VDOM license key

1. Log in with a super_admin account.
2. Go to the **Dashboard**.
3. Record your FortiGate serial number as shown in **System Information** widget.
4. In the **License Information** widget, locate **Virtual Domain** and select **Purchase More**.

If you don't see the **Purchase More** option, your FortiGate model does not support more than 10 VDOMs.

5. You are directed to the Fortinet Support website, where you can log in and purchase a license key.
6. After you receive your license key, go to the Dashboard and select **Upload License** under **License Information**, **Virtual Domains**.
7. In the **Input License Key** field, enter the license key you received from Fortinet Support.
8. Select **Apply**.

To verify the new VDOM license, in global configuration go to **System > Dashboard**. The **Licenses** widget shows the current number and total allowed number of VDOMs.

Configuring additional VDOMs

This section contains the following topics:

- Creating a VDOM
- Changing the management VDOM
- Assigning interfaces to a VDOM

- Per-VDOM administrators
- Certificate management
- Security profiles
- Disabling a VDOM
- Deleting a VDOM

Creating a VDOM

FortiGate performance might be reduced if you create a large number of VDOMs.

To create new VDOMs, you must use a super_admin profile account and connect to the management VDOM (the root VDOM, by default).

By default, new VDOMs are set to NAT mode. If you want a VDOM to be in transparent mode, you must manually change the operation mode using the CLI. For more information, see the Transparent mode Handbook.

To create a VDOM - GUI:

1. Connect to the management VDOM.
2. Go to **Global > System > VDOM** and select **Create New**.
3. Enter a unique **Name**. VDOM names have the following restrictions:
   - Only letters, numbers, "-", and "_" are allowed
   - No more than 11 characters are allowed
   - No spaces are allowed
   - VDOMs can't have the same names as interfaces, zones, switch interfaces, or other VDOMs
4. Enter a short and descriptive comment to identify this VDOM.
5. Select **OK**.

To create a VDOM - CLI:

```
config system vdom
   edit <new_vdom_name>
end
```

If you attempt to edit an existing VDOM in the CLI and mistype the name, a new VDOM is created with this name.

The new VDOM can either be renamed or deleted. For more information, see Deleting a VDOM.

Changing the management VDOM

You can't change the management VDOM if any administrators are using RADIUS authentication.

Once you have two or more VDOMs, you can change the management VDOM. The management VDOM must have Internet access.

You use the management VDOM to access global settings on the FortiGate, as well as for the following services:

- DNS lookups
- Logging to a FortiAnalyzer or syslog
- FortiGuard service
- Sending alert emails
- Network time protocol traffic (NTP)
- Sending SNMP traps
- Quarantining suspicious files and email

To change the management VDOM - GUI:

1. Select **Global > System > VDOM.**
2. Select the new management VDOM.
3. Select **Switch Management**.
4. Select **OK** to confirm the change.

To change the management VDOM - CLI:

```
config global
   config system global
      set management-vdom <vdom_name>
   end
end
```

Assigning interfaces to a VDOM

You can assign an interface to only a single VDOM. By default, all interfaces are assigned to the root VDOM.

If the existing configuration references an interface, you won't be able to change the VDOM assignment for that interface. Because some FortiGate models have a default configuration, you might need to delete existing policies and routes to assign a particular interface to a new VDOM.

To assign an interface to a VDOM - GUI:

1. Connect to the management VDOM.
2. Go to **Global > Network > Interfaces** and edit the interface.
3. Set **Virtual Domain** to the appropriate VDOM.
4. Select **OK**.

To assign an interface to a VDOM - CLI:

```
config global
   config system interface
      edit <interface_name>
         set vdom <VDOM_name>
      next
   end
end
```

If you want to use the same physical interface for multiple VDOMs, you can use an enhanced MAC VLAN. For more information, see the Networking Handbook.

Per-VDOM administrators

After you enable VDOMs, you can create administrators with access to several VDOMs or limited to a single VDOM, called per-VDOM administrators.

Per-VDOM administrators must have either the prof_admin profile or a custom profile. Administrators who have the super_admin profile have access to all VDOMs on the FortiGate. For more information, see the System Administration handbook.

Per-VDOM administrators must access the FortiGate through network interfaces that belong to those VDOMs, which must be configured to allow management access. The administrator can also connect using the console interface.

When per-VDOM administrators log into their virtual domain, they see a different dashboard than the global administrator sees. The VDOM dashboard displays information only relevant to that VDOM, while information about global settings or other VDOMs aren't shown.

Information	Per-VDOM	Global
System information	read-only	yes
License information	no	yes
CLI console	yes	yes
Unit operation	read-only	yes
Alert message console	no	yes
Top sessions	limited to VDOM sessions	yes
Traffic	limited to VDOM interfaces	yes
Statistics	yes	yes

You can create administrators globally or per-VDOM. To assign an administrator to multiple VDOMs, you must create the account at the global level.

When creating an administrator at the per-VDOM level, the super_admin profile can't be used.

To create per-VDOM administrators - GUI:

1. Connect to the management VDOM.
2. Go to **Global > System > Administrators** and select **Create New**.
3. Set the **User Name** for the account.
4. Set and confirm the **Password**.
5. Set **Type** to **Local User**.
6. Remove the **root** VDOM from the **Virtual Domains** list, then add the appropriate VDOM.
7. Select **OK**.

To create per-VDOM administrators - CLI:

```
config global
   config system admin
      edit <name>
         set vdom <VDOM_name>
         set password <password>
         set accprofile <admin_profile>
         ...
      next
   end
end
```

Certificate management

The following factory default certificates are unique to each VDOM and are automatically generated when a new VDOM is added:

- Fortinet_CA_SSL
- Fortinet_SSL
- PositiveSSL_CA
- Fortinet_Wifi
- Fortinet_Factory

You can upload certificates to either the global certificate store or the certificate store for a specific VDOM. Global certificates are available to all VDOMs on the FortiGate, while VDOM certificates are available only for a single VDOM.

Security profiles

A single VDOM can use all the security features that are available to a FortiGate that does not use VDOMs.

When applying security profiles, you can use global security profiles, which are available for use by multiple VDOMs, as well as VDOM-level security profiles. Both types of profiles can be used together on the same VDOM.

VDOM-level security profiles

If you create a security profile on a specific VDOM, that profile is only available on that VDOM. When using a global administrator account, you can create, edit, and delete VDOM-level security profiles by using the drop-down menu to access the VDOM, then going to the **Security Profiles** menu.

Global security profiles

You can configure global security profiles for use by multiple VDOMs, to avoid creating identical profiles for each VDOM individually. Global profiles are available for the following security features:

- Antivirus
- Application control
- Data leak prevention
- Intrusion protection
- Web filtering

Some security profile features, such as URL filters, are not available for use in a global profile.

The name for any global profile must start with "g-" for identification. Global profiles are available as read-only for VDOM-level administrators and can only be edited or deleted from within the global settings. Each security feature has at least one default global profile.

Global profiles are configured by going to **Global > Security Profiles** in the GUI or under the following `config global` commands in the CLI:

- `antivirus profile`
- `application list`
- `dlp sensor`
- `ips sensor`
- `webfilter profile`

Disabling a VDOM

When you create a new VDOM, it's enabled by default. You can configure a VDOM only while it is enabled. You must enable the management VDOM.

Disabled VDOMs are considered offline. The configuration remains, but you can't use the VDOM and only the super_admin administrator can view it. You can assign interfaces to a disabled VDOM.

To disable a VDOM - GUI:

1. Go to **Global > System > VDOM**.
2. Open the VDOM for editing.
3. Ensure **Enable** is not selected.
4. Select **OK**.

To disable a VDOM - CLI:

```
config vdom
   edit <name>
      config system settings
         set status disable
      end
end
```

Deleting a VDOM

Deleting a VDOM removes it from the FortiGate configuration. You can't delete the root VDOM or the management VDOM, and you can't delete a disabled VDOM.

You can delete only VDOMs that aren't referenced by the current configuration, including any per-VDOM objects. Before you delete a VDOM, check for, and remove the following objects that refer to that VDOM or its components:

- Routing - both static and dynamic routes
- Firewall addresses, policies, groups, or other settings
- Security profiles
- VPN configuration
- Users or user groups
- Logging
- DHCP servers
- Network interfaces, zones, and custom DNS servers
- VDOM administrators

Before you delete a VDOM, it's recommended that you re-assign interfaces assigned to that VDOM to the root VDOM.

To delete a VDOM - GUI:

1. Go to **Global > System > VDOM**.
2. Select the check box for the VDOM and then select the **Delete** icon.
3. Confirm the deletion.

To delete a VDOM - CLI:

```
config vdom
   delete test-vdom
end
```

Inter-VDOM routing

Inter-VDOM routing allows two VDOMs on the same FortiGate to communicate internally. Traffic between VDOMs flows through an inter-VDOM link, which contains a pair of virtual interfaces, one on each VDOM.

Inter-VDOM routing isn't supported when both VDOMs use transparent mode.

Types of inter-VDOM links

The virtual interfaces in an inter-VDOM links don't require IP addresses by default, because the interfaces are internal connections that can be referred to by name in firewall policies and other system references. However, some network configurations require assigned IP addresses for the virtual interfaces,

There are three types of inter-VDOM link, depending on whether or not the virtual interfaces have assigned IP addresses:

- **Unnumbered** - neither interfaces have an IP address
- **Half numbered** - only one of the interfaces has an IP address
- **Full numbered** - both interfaces have an IP address

Static routing

You can use unnumbered inter-VDOM links in static routing by naming the interface and using `0.0.0.0` for the gateway. Running traceroute will not show the interface in the list of hops. However, you can see the interface during packet sniffing, which is useful for troubleshooting. However, if NAT is applied to internal traffic, IP addresses might be required.

Dynamic routing

Dynamic routing using inter-VDOM links must be point to point.

In dynamic routing, the types of inter-VDOM link you can use depends on the routing protocol, as shown below. In general, you should use numbered inter-VDOM links for dynamic routing.

Routing protocol	Unnumbered	Half numbered	Full numbered
BGP	No	No	Yes
OSPF	Yes, but not recommended	Yes, but not recommended	Yes
RIP	Yes, but not recommended	Yes, but not recommended	Yes
Multicast	Yes, but the virtual interfaces are unable to become RP candidates	Yes, but the virtual interface without an IP address is unable to become an RP candidate	Yes

HA virtual clusters

Inter-VDOM links can be used to extend FortiGate high availability (HA) and provide failover protection and load balancing for a FortiGate operating with VDOMs. An HA cluster that includes VDOMs is known as a virtual cluster, or vcluster

Virtual clusters can operate in active-passive or active-active HA mode for clusters of up to four FortiGates. Active-passive virtual clustering includes VDOM partitioning to distribute traffic for different VDOMs between the primary and backup FortiGates.

For more information about virtual clusters, see the High Availability Handbook.

Creating inter-VDOM links

Inter-VDOM links are a global setting and you must use a global administrator account to create them.

The process to create an inter-VDOM link depends on the operation mode of the VDOMs.

NAT-to-NAT routing

If both VDOMs use NAT mode, you can create an inter-VDOM link using either the GUI or CLI.

To configure an inter-VDOM link - GUI:

1. Go to **Global > Network > Interfaces**.
2. Select **Create New > VDOM link**.
3. Assign a **Name** to the link. This name is also used for the two virtual interfaces, with a 0 or 1 appended to the end.
4. Under **Interface 0**, set the **Virtual Domain** and, if required, set an **IP/Netmask**.
5. Under **Interface 1**, set the **Virtual Domain** and, if required, set an **IP/Netmask**.
6. Select **OK**.

To configure an inter-VDOM link - CLI:

```
config global
   config system vdom-link
      edit <name>
   end
   config system interface
      edit <name>
         set vdom <VDOM>
         set ip <address> <netmask>
      next
      edit <name>
         set vdom <VDOM>
         set ip <address> <netmask>
      next
   end
```

To confirm that the inter-VDOM link was created, go to **Network > Interfaces** and locate the inter-VDOM link. Expand the link to view the virtual interfaces.

After you create the inter-VDOM link, configure firewall policies and other settings to allow traffic to flow between the two VDOMs.

NAT-to-transparent routing

You must use the CLI to create inter-VDOM links between a VDOM in NAT mode and a VDOM in transparent mode, because the inter-VDOM link `type` must be changed to `ethernet`. This configuration also requires a half numbered inter-VDOM link, with an IP address assigned to the virtual interface on the NAT VDOM. The virtual interface on the transparent VDOM doesn't have an IP address.

To configure a NAT-to-transparent VDOM link:

```
config global
   config system vdom-link
      edit <name>
         set type ethernet
      end
   config system interface
      edit <name>
         set vdom <NAT_VDOM>
         set ip <address> <netmask>
      next
      edit <name>
         set vdom <transparent_VDOM>
      next
   end
```

To confirm that the inter-VDOM link was created, go to **Network > Interfaces** and locate the inter-VDOM link. Expand the link to view the virtual interfaces.

After you create the inter-VDOM link, configure firewall policies and other settings to allow traffic to flow between the two VDOMs.

Deleting VDOM links

Before deleting the VDOM link, ensure all policies, firewalls, and other configurations that include the VDOM link are deleted, removed, or changed to no longer include the VDOM link.

When you delete the VDOM link, you also delete the virtual interfaces. You can't delete the virtual interfaces individually.

To remove a VDOM link - GUI:

1. Go to **Global > Network > Interfaces**.
2. Select the VDOM link.
3. Select **Delete**.
4. When prompted, select **OK**.

To remove a VDOM link - CLI:

```
config global
   config system vdom-link
      delete <name>
   end
```

VDOMs in NAT mode

By default, VDOMs operate in NAT mode. In this mode, you install the VDOM as a gateway or router between two networks, typically a private network and the Internet. In this configuration, the VDOM uses network address translation (NAT) to hide the private IP addresses of network devices.

You can use VDOMs in NAT mode and transparent mode together on the same FortiGate. For more information about transparent mode, see "VDOMs in transparent mode" on page 39.

This chapter contains the following sections:

- Using a VDOM in NAT/route mode
- Example configuration: VDOM in NAT/route mode

Using a VDOM in NAT/route mode

This section contains information about how to configure a VDOM in NAT/route mode, including the following:

- Configuring VDOM routing
- Configuring security policies
- Changing the inspection mode
- Using a VDOM in NAT/route mode
- Configuring VPNs for a VDOM
- Using a VDOM in NAT/route mode

Configuring VDOM routing

Routing is VDOM-specific. Each VDOM should have a default static route configured as a minimum. Within a VDOM, routing is the same as routing on your FortiGate without VDOMs enabled.

When configuring dynamic routing on a VDOM, other VDOMs on the FortiGate can be neighbors. The following topics give a brief introduction to the routing protocols, and show specific examples of how to configure dynamic routing for VDOMs. Figures are included to show the FortiGate configuration after the successful completion of the routing example.

Default static route for a VDOM

The routing you define applies only to network traffic entering non-ssl interfaces belonging to this VDOM. Set the administrative distance high enough, typically 20, so that automatically configured routes will be preferred to the default.

In the following procedure, it is assumed that a VDOM called “Client2” exists. The procedure will create a default static route for this VDOM. The route has a destination IP of 0.0.0.0, on the port3 interface. It has a gateway of 10.10.10.1, and an administrative distance of 20.

The values used in this procedure are very standard, and this procedure should be part of configuring all VDOMs.

To add a default static route for a VDOM - GUI:

1. In **Virtual Domains**, select the client2 VDOM.
2. Go to **Network > Static Routes**.
3. Select **Create New**.
4. Enter the following information and select **OK**:

Destination IP/Mask	0.0.0.0/0.0.0.0
Device	port2
Gateway	10.10.10.1
Distance	20

To add a default static route for a VDOM - CLI:

```
config vdom
   edit client2
      config router static
         edit 4
            set device port2
            set dst 0.0.0.0 0.0.0.0
            set gateway 10.10.10.1
            set distance 20
         end
   end
```

Dynamic routing in VDOMs

Dynamic routing is VDOM-specific, like all other routing. Dynamic routing configuration is the same with VDOMs as with your FortiGate without VDOMs enabled, once you're at the routing menu. If you have multiple VDOMs configured, the dynamic routing configuration between them can become quite complex.

VDOMs provide some interesting changes to dynamic routing. Each VDOM can be a neighbor to the other VDOMs. This is useful in simulating a dynamic routing area or AS or network using only your FortiGate.

You can separate different types of routing to different VDOMs if required. This allows for easier troubleshooting. This is very useful if your FortiGate is on the border of a number of different routing domains.

For more information on dynamic routing in FortiOS, see the *Networking Handbook*.

Inter-VDOM links must have IP addresses assigned to them if they are part of a dynamic routing configuration. Inter-VDOM links may or may not have IP addresses assigned to them. Without IP addresses, you need to be careful how you configure routing. While the default static route can be assigned an address of 0.0.0.0 and rely instead on the interface, dynamic routing almost always requires an IP address.

RIP

The RIP dynamic routing protocol uses hop count to determine the best route, with a hop count of 1 being directly attached to the interface and a hop count of 16 being unreachable. For example if two VDOMs on the same FortiGate are RIP neighbors, they have a hop count of 1.

OSPF

OSPF communicates the status of its network links to adjacent neighbor routers instead of the complete routing table. When compared to RIP, OSPF is more suitable for large networks, it is not limited by hop count, and is more complex to configure. For smaller OSPF configurations its easiest to just use the backbone area, instead of multiple areas.

BGP

BGP is an Internet gateway protocol (IGP) used to connect autonomous systems (ASes) and is used by Internet service providers (ISPs). BGP stores the full path, or path vector, to a destination and its attributes which aid in proper routing.

Configuring security policies

Security policies are VDOM-specific. This means that all firewall settings for a VDOM, such as firewall addresses and security policies, are configured within the VDOM.

In VDOMs, all firewall related objects are configured per-VDOM including addresses, service groups, security profiles, schedules, traffic shaping, and so on. If you want firewall addresses, you will have to create them on each VDOM separately. If you have many addresses, and VDOMs this can be tedious and time consuming. Consider using a FortiManager unit to manage your VDOM configuration — it can get firewall objects from a configured VDOM or FortiGate, and push those objects to many other VDOMs or FortiGate devices. See the FortiManager Administration Guide.

You can customize the **Policy** display by including some or all columns, and customize the column order onscreen. Due to this feature, security policy screen shots may not appear the same as on your screen.

Configuring a security policy for a VDOM

Your security policies can involve only the interfaces, zones, and firewall addresses that are part of the current VDOM, and they are only visible when you're viewing the current VDOM. The security policies of this VDOM filter the network traffic on the interfaces and VLAN subinterfaces in this VDOM.

A firewall service group can be configured to group multiple services into one service group. When a descriptive name is used, service groups make it easier for an administrator to quickly determine what services are allowed by a security policy.

In the following procedure, it is assumed that a VDOM called `Client2` exists. The procedure will configure an outgoing security policy. The security policy will allow all HTTPS, SSH, and DNS traffic for the `SalesLocal` address group on VLAN_200 going to all addresses on port3. This traffic will be scanned and logged.

To configure a security policy for a VDOM - GUI:

1. In **Virtual Domains**, select the client2 VDOM.
2. Go to **Policy & Objects > IPv4 Policy**.
3. Select **Create New**.
4. Enter the following information and select **OK**:

Name	Client2-outgoing
Incoming Interface	VLAN_200
Outgoing Interface	port3
Source Address	SalesLocal
Destination Address	any
Schedule	always
Service	HTTPS, SSH, DNS
Action	ACCEPT
Log Allowed Traffic	enable

To configure a security policy for a VDOM - CLI:

```
config vdom
   edit Client2
      config firewall policy
         edit 12
            set srcintf VLAN_200
            set srcaddr SalesLocal
            set dstintf port3
            set dstaddr any
            set schedule always
            set service HTTPS SSH
            set action accept
            set status enable
            set logtraffic enable
         end
   end
```

Changing the inspection mode

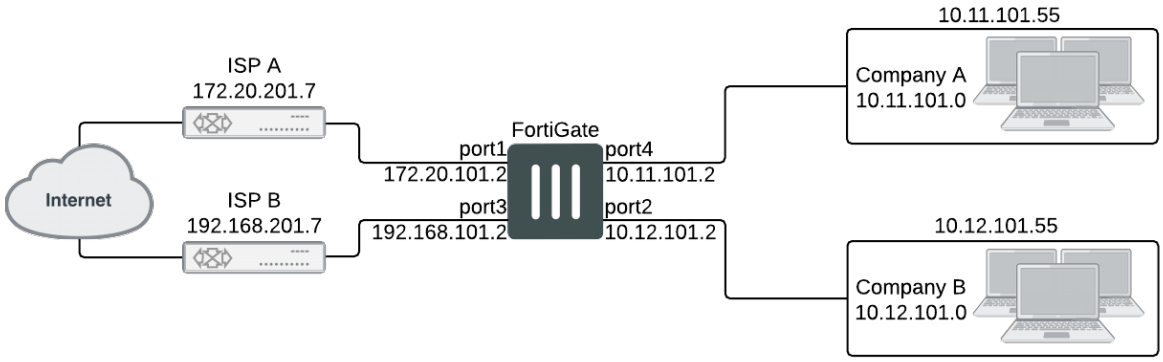
If you wish to change the inspection mode for a VDOM, go to **System > VDOM** and edit the VDOM you want to configure. Set **Inspection Mode** to either **Proxy** or **Flow-based**.

VDOMs on the same FortiGate can use different inspection modes.

Configuring VPNs for a VDOM

Virtual Private Networking (VPN) settings are VDOM-specific, and must be configured within each VDOM. Configurations for IPsec Tunnel, IPsec Interface, PPTP and SSL are VDOM-specific.

Example configuration: VDOM in NAT/route mode



Company A and Company B each have their own internal networks and their own ISPs. They share a FortiGate that is configured with two separate VDOMs, with each VDOM running in NAT/route mode enabling separate configuration of network protection profiles. Each ISP is connected to a different interface on the FortiGate.

This network example was chosen to illustrate one of the most typical VDOM configurations.

This example has the following sections:

- Network topology and assumptions
- General configuration steps
- Creating the VDOMs
- Configuring the FortiGate interfaces
- Configuring the vdomA VDOM
- Configuring the vdomB VDOM
- Testing the configuration

Network topology and assumptions

Both companies have their own ISPs and their own internal interface, external interface, and VDOM on the FortiGate.

For easier configuration, the following IP addressing is used:

- all IP addresses on the FortiGate end in ".2" such as 10.11.101.2.
- all IP addresses for ISPs end in ".7", such as 172.20.201.7.
- all internal networks are 10.*.*.* networks, and sample internal addresses end in ".55".

The IP address matrix for this example is as follows.

Address	Company A	Company B
ISP	172.20.201.7	192.168.201.7
Internal network	10.11.101.0	10.012.101.0

Address	Company A	Company B
FortiGate / VDOM	`172.20.201.2 (port1)` `10.11.101.2 (port4)`	`192.168.201.2 (port3)` `10.012.101.2 (port2)`

The Company A internal network is on the 10.11.101.0/255.255.255.0 subnet. The Company B internal network is on the 10.12.101.0/255.255.255.0 subnet.

There are no switches or routers required for this configuration.

There are no VLANs in this network topology.

The interfaces used in this example are port1 through port4. Different FortiGate models may have different interface labels. port1 and port3 are used as external interfaces. port2 and port4 are internal interfaces.

The administrator is a super_admin account. If you're a using a non-super_admin account, refer to "Global and per-VDOM settings" to see which parts a non-super_admin account can also configure.

When configuring security policies in the CLI always choose a policy number that is higher than any existing policy numbers, select `services` before `profile-status`, and `profile-status` before `profile`. If these commands are not entered in that order, they may not be available to enter.

General configuration steps

For best results in this configuration, follow the procedures in the order given. Also, note that if you perform any additional actions between procedures, your configuration may have different results.

1. Creating the VDOMs
2. Configuring the FortiGate interfaces
3. Configuring the vdomA VDOM, and Configuring the vdomB VDOM
4. Testing the configuration

Creating the VDOMs

In this example, two new VDOMs are created — vdomA for Company A and vdomB for Company B. These VDOMs will keep the traffic for these two companies separate while enabling each company to access its own ISP.

To create two VDOMs - GUI:

1. Log in with a super_admin account.
2. Go to **Global > System > VDOM**, and select **Create New**.
3. Enter `vdomA` and select **OK**.
4. Select **OK** again to return to the VDOM list.
5. Select **Create New**.
6. Enter `vdomB` and select **OK**.

To create two VDOMs - CLI:

```
config vdom
   edit vdomA
```

```
    next
    edit vdomB
end
```

Configuring the FortiGate interfaces

This section configures the interfaces that connect to the companies' internal networks, and to the companies' ISPs.

All interfaces on the FortiGate will be configured with an IP address ending in ".2" such as 10.11.101.2. This will simplify network administration both for the companies, and for the FortiGate global administrator. Also the internal addresses for each company differ in the second octet of their IP address - Company A is 10.11.*, and Company B is 10.12.*.

This section includes the following topics:

- Configuring the vdomA interfaces
- Configuring the vdomB interfaces

If you can't change the VDOM of an network interface it is because something is referring to that interface that needs to be deleted. Once all the references are deleted the interface will be available to switch to a different VDOM. For example a common reference to the external interface is the default static route entry. See Example configuration: VDOM in NAT/route mode.

Configuring the vdomA interfaces

The `vdomA` VDOM includes two FortiGate interfaces: port1 and external.

The port4 interface connects the Company A internal network to the FortiGate, and shares the internal network subnet of 10.11.101.0/255.255.255.0.

The external interface connects the FortiGate to ISP A and the Internet. It shares the ISP A subnet of 172.20.201.0/255.255.255.0.

To configure the vdomA interfaces - GUI:

1. Go to **Global > Network > Interfaces**.
2. Select **Edit** on the port1 interface.
3. Enter the following information and select **OK**:

Virtual Domain	vdomA
Addressing mode	Manual
IP/Netmask	172.20.201.2/255.255.255.0

4. Select **Edit** on the port4 interface.
5. Enter the following information and select **OK**:

Virtual Domain	vdomA

Addressing mode	Manual
IP/Netmask	10.11.101.2/255.255.255.0

To configure the vdomA interfaces - CLI:

```
config global
   config system interface
      edit port1
         set vdom vdomA
         set mode static
         set ip 172.20.201.2 255.255.255.0
      next
      edit port4
         set vdom ABCDomain
         set mode static
         set ip 10.11.101.2 255.255.255.0
      end
```

Configuring the vdomB interfaces

The `vdomB` VDOM uses two FortiGate interfaces: port2 and port3.

The port2 interface connects the Company B internal network to the FortiGate, and shares the internal network subnet of 10.12.101.0/255.255.255.0.

The port3 interface connects the FortiGate to ISP B and the Internet. It shares the ISP B subnet of 192.168.201.0/255.255.255.0.

To configure the vdomB interfaces - GUI:

1. Go to **Global > Network > Interfaces**.
2. Select **Edit** on the port3 interface.
3. Enter the following information and select **OK**:

Virtual domain	vdomB
Addressing mode	Manual
IP/Netmask	192.168.201.2/255.255.255.0

4. Select **Edit** on the port2 interface.
5. Enter the following information and select **OK**:

Virtual domain	vdomB
Addressing mode	Manual
IP/Netmask	10.12.101.2/255.255.255.0

To configure the vdomB interfaces - CLI:

```
config global
   config system interface
```

```
      edit port3
         set vdom vdomB
         set mode static
         set ip 192.168.201.2 255.255.255.0
      next
      edit port2
         set vdom vdomB
         set mode static
         set ip 10.12.101.2 255.255.255.0
   end
```

Configuring the vdomA VDOM

With the VDOMs created and the ISPs connected, the next step is to configure the vdomA VDOM.

Configuring the vdomA includes the following:

- Adding vdomA firewall addresses
- Adding the vdomA security policy
- Adding the vdomA default route

Adding vdomA firewall addresses

You need to define the addresses used by Company A's internal network for use in security policies. This internal network is the 10.11.101.0/255.255.255.0 subnet.

The FortiGate provides one default address, "all", that you can use when a security policy applies to all addresses as the source or destination of a packet.

To add the vdomA firewall addresses - GUI:

1. In **Virtual Domains**, select **vdomA**.
2. Go to **Policy & Objects > Addresses**.
3. Select **Create New**.
4. Enter the following information and select **OK**:

Address Name	Ainternal
Type	Subnet / IP Range
Subnet / IP Range	10.11.101.0/255.255.255.0
Interface	port4

To add the ABCDomain VDOM firewall addresses - CLI:

```
config vdom
   edit vdomA
      config firewall address
         edit Ainternal
            set type ipmask
            set subnet 10.11.101.0 255.255.255.0
      end
   end
```

Adding the vdomA security policy

You need to add the `vdomA` security policy to allow traffic from the internal network to reach the external network, and from the external network to internal as well. You need two policies for this domain.

To add the vdomA security policy - GUI:

1. In **Virtual Domains**, select **vdomA**.
2. Go to **Policy & Objects > IPv4 Policy**.
3. Select **Create New**.
4. Enter the following information and select **OK**:

Name	VDOMA-internal-to-external
Incoming Interface	port4
Outgoing Interface	port1
Source Address	Ainternal
Destination Address	all
Schedule	Always
Service	ANY
Action	ACCEPT

5. Select **Create New**.
6. Enter the following information and select **OK**:

Name	VDOMA-external-to-internal
Incoming Interface	port1
Outgoing Interface	port4
Source Address	all
Destination Address	Ainternal
Schedule	Always
Service	ANY
Action	ACCEPT

To add the vdomA security policy - CLI:

```
config vdom
   edit vdomA
      config firewall policy
         edit 1
            set srcintf port4
            set srcaddr Ainternal
```

```
      set dstintf port1
      set dstaddr all
      set schedule always
      set service ANY
      set action accept
      set status enable
   next
   edit 2
      set srcintf port1
      set srcaddr all
      set dstintf port4
      set dstaddr Ainternal
      set schedule always
      set service ANY
      set action accept
      set status enable
   end
```

Adding the vdomA default route

You also need to define a default route to direct packets from the Company A internal network to ISP A. Every VDOM needs a default static route, as a minimum, to handle traffic addressed to external networks such as the Internet.

The administrative distance should be set slightly higher than other routes. Lower admin distances will get checked first, and this default route will only be used as a last resort.

To add a default route to the vdomA - GUI:

1. For **Virtual Domains**, select **vdomA**
2. Go to **Network > Static Routes**.
3. Select **Create New**.
4. Enter the following information and select **OK**:

Destination IP/Mask	0.0.0.0/0.0.0.0
Device	port1
Gateway	172.20.201.7
Distance	20

To add a default route to the vdomA - CLI:

```
config vdom
   edit vdomA
      config router static
         edit 1
            set device port1
            set gateway 172.20.201.7
         end
```

Configuring the vdomB VDOM

In this example, the vdomB VDOM is used for Company B. Firewall and routing settings are specific to a single VDOM.

vdomB includes the FortiGate port2 interface to connect to the Company B internal network, and the FortiGate port3 interface to connect to ISP B. Security policies are needed to allow traffic from port2 to external and from external to port2 interfaces.

This section includes the following topics:

- Adding the vdomB firewall address
- Adding the vdomB security policy
- Adding a default route to the vdomB VDOM

Adding the vdomB firewall address

You need to define addresses for use in security policies. In this example, the vdomB VDOM needs an address for the port2 interface and the “all” address.

To add the vdomB firewall address - GUI:

1. In **Virtual Domains**, select **vdomB**.
2. Go to **Policy & Objects > Addresses**.
3. Select **Create New**.
4. Enter the following information and select **OK**:

Address Name	Binternal
Type	Subnet / IP Range
Subnet / IP Range	10.12.101.0/255.255.255.0
Interface	port2

To add the vdomB firewall address - CLI:

```
config vdom
   edit vdomB
      config firewall address
         edit Binternal
            set type ipmask
            set subnet 10.12.101.0 255.255.255.0
         end
   end
```

Adding the vdomB security policy

You also need a security policy for the Company B domain. In this example, the security policy allows all traffic.

To add the vdomB security policy - GUI:

1. Log in with a super_admin account.
2. In **Virtual Domains**, select vdomB.
3. Go to **Policy & Objects > IPv4 Policy**
4. Select **Create New**.
5. Enter the following information and select **OK**:

Name	VDOMB-internal-to-external
Incoming Interface	port2
Outgoing Interface	port3
Source Address	Binternal
Destination Address	all
Schedule	Always
Service	ANY
Action	ACCEPT

6. Select **Create New**.
7. Enter the following information and select **OK**:

Name	VDOMB-external-to-internal
Incoming Interface	port3
Outgoing Interface	port2
Source Address	all
Destination Address	Binternal
Schedule	Always
Service	ANY
Action	ACCEPT

To add the vdomB security policy - CLI:

```
config vdom
   edit vdomB
      config firewall policy
         edit 1
            set srcintf port2
            set dstintf port3
            set srcaddr Binternal
            set dstaddr all
            set schedule always
            set service ANY
```

```
            set action accept
            set status enable
        edit 1
            set srcintf port3
            set dstintf port2
            set srcaddr all
            set dstaddr Binternal
            set schedule always
            set service ANY
            set action accept
            set status enable
        end
end
```

Adding a default route to the vdomB VDOM

You need to define a default route to direct packets to ISP B.

To add a default route to the vdomB VDOM - GUI:

1. Log in as the super_admin administrator.
2. In **Virtual Domains**, select vdomB.
3. Go to **Network > Static Routes**.
4. Select **Create New**.
5. Enter the following information and select **OK**:

Destination IP/Mask	0.0.0.0/0.0.0.0
Device	port3
Gateway	192.168.201.7
Distance	20

To add a default route to the vdomB VDOM - CLI:

```
config vdom
   edit vdomB
      config router static
         edit 1
            set dst 0.0.0.0/0
            set device external
            set gateway 192.168.201.7
         end
   end
```

Testing the configuration

Once you have completed configuration for both company VDOMs, you can use diagnostic commands, such as `tracert` in Windows, to test traffic routed through the FortiGate. Alternately, you can use the `traceroute` command on a Linux system with similar output.

Possible errors during the traceroute test are:

- "`* * * Request timed out`" - the trace was not able to make the next connection towards the destination fast enough
- "`Destination host unreachable`" - after a number of timed-out responses the trace will give up

Possible reasons for these errors are bad connections or configuration errors.

For additional troubleshooting, see Troubleshooting VDOMs.

Testing traffic from the internal network to the ISP

In this example, a route is traced from the Company A internal network to ISP A. The test was run on a Windows PC with an IP address of 10.11.101.55.

The output here indicates three hops between the source and destination, the IP address of each hop, and that the trace was successful.

From the Company A internal network, access a command prompt and enter this command:

```
C:\>tracert 172.20.201.7
Tracing route to 172.20.201.7 over a maximum of 30 hops:
  1   <10 ms   <10 ms   <10 ms  10.11.101.2
  2   <10 ms   <10 ms   <10 ms  172.20.201.2
  3   <10 ms   <10 ms   <10 ms  172.20.201.7
Trace complete.
```

VDOMs in transparent mode

A VDOM in transparent mode is installed between the internal network and the router. In this mode, the VDOM does not make any changes to IP addresses and only applies security scanning to traffic. When a VDOM is added to a network in transparent mode, no network changes are required, except to provide the VDOM with a management IP address.

Each VDOM on a FortiGate can be configured for NAT/route mode or transparent mode, regardless of the operation mode of other VDOMs on the FortiGate. For more information about NAT/route mode, see "VDOMs in NAT mode" on page 24.

This chapter includes the following sections:

- VDOMs in transparent mode
- Using a VDOM in transparent mode
- VDOMs in transparent mode

VDOMs in transparent mode

A VDOM, such as root, can have a maximum of 255 interfaces in Network Address Translation (NAT) mode or transparent mode. This includes VLANs, other virtual interfaces, and physical interfaces. To have more than a total of 255 interfaces configured, you need multiple VDOMs with multiple interfaces on each.

In transparent mode without VDOMs enabled, all interfaces on the FortiGate act as a bridge — all traffic coming in on one interface is sent back out on all the other interfaces. This effectively turns the FortiGate into a two interface unit no matter how many physical interfaces it has. When VDOMs are enabled, this allows you to determine how many interfaces to assign to a VDOM running in transparent mode. If there are reasons for assigning more than two interfaces based on your network topology, you're able to. However, the benefit of VDOMs in this case is that you have the functionality of transparent mode, but you can use interfaces for NAT/route traffic as well.

You can add more VDOMs to separate groups of VLAN subinterfaces. When using a FortiGate to serve multiple organizations, this configuration simplifies administration because you see only the security policies and settings for the VDOM you're configuring.

One essential application of VDOMs is to prevent problems caused when a FortiGate is connected to a layer-2 switch that has a global MAC table. FortiGate devices normally forward ARP requests to all interfaces, including VLAN subinterfaces. It is then possible for the switch to receive duplicate ARP packets on different VLANs. Some layer-2 switches reset when this happens. As ARP requests are only forwarded to interfaces in the same VDOM, you can solve this problem by creating a VDOM for each VLAN.

For more information about transparent mode, see the *Transparent Mode Handbook*.

Using a VDOM in transparent mode

The essential steps to configure a VDOM in transparent mode are:

- Switching to transparent mode
- Adding VLAN subinterfaces
- Creating security policies

You can also configure the security profiles that manage antivirus scanning, web filtering and spam filtering.

In transparent mode, you can access the GUI by connecting to an interface configured for administrative access and using HTTPS to access the management IP address. In the following examples, administrative access is enabled by default on the internal interface and the default management IP address is `10.11.0.1`.

Switching to transparent mode

A VDOM is in NAT/route mode by default when it is created. You must switch it to transparent mode, and add a management IP address so you can access the VDOM from your management computer.

Before applying the change to transparent mode, ensure the VDOM has administrative access on the selected interface, and that the selected management IP address is reachable on your network.

Switching the VDOM to transparent mode can't be done through the GUI. It must be done through the CLI only.

To switch the VDOM to transparent mode - CLI:

```
config vdom
   edit <name>
      config system settings
         set opmode transparent
         set mangeip 10.11.0.99 255.255.255.0
      end
   end
```

Adding VLAN subinterfaces

There are a few differences when adding VLANs in transparent mode compared to NAT/route mode.

In transparent mode, VLAN traffic is trunked across the VDOM. That means VLAN traffic can't be routed, changed, or inspected. For this reason when you assign a VLAN to a transparent mode VDOM, you will see the **Addressing Mode** section of the interface configuration disappear in from the GUI. It is because with no routing, inspection, or any activities able to be performed on VLAN traffic the VDOM simply re-broadcasts the VLAN traffic. This requires no addressing.

Also any routing related features such as dynamic routing or Virtual Router Redundancy Protocol (VRRP) are not available in transparent mode for any interfaces.

Creating security policies

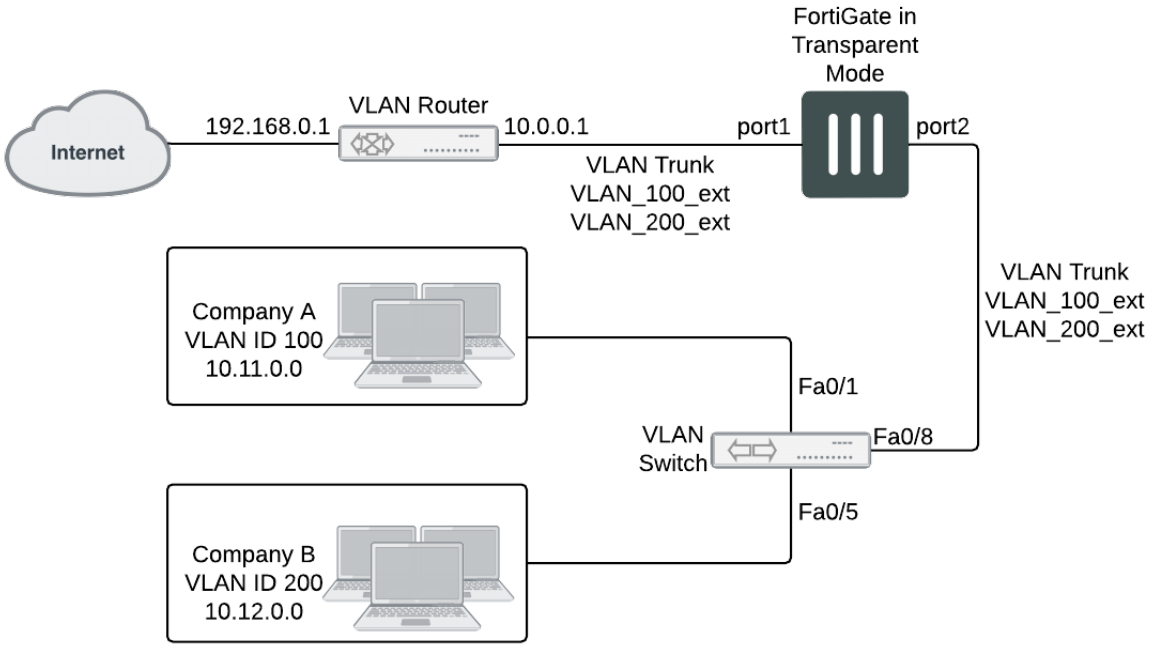
Security policies permit communication between the FortiGate's network interfaces based on source and destination IP addresses. Typically you will also limit communication to desired times and services for additional security.

In transparent mode, the FortiGate performs antivirus and antispam scanning on each packet as it passes through the unit. You need security policies to permit packets to pass from the VLAN interface where they enter

the unit to the VLAN interface where they exit the unit. If there are no security policies configured, no packets will be allowed to pass from one interface to another.

For more information, see the Firewall handbook.

Example configuration: VDOM in transparent mode



In this example, the FortiGate provides network protection to two organizations — Company A and Company B. Each company has different policies for incoming and outgoing traffic, requiring three different security policies and protection profiles.

VDOMs are not required for this configuration, but by using VDOMs the profiles and policies can be more easily managed on a per-VDOM basis either by one central administrator or separate administrators for each company. Also future expansion is simply a matter of adding additional VDOMs, whilst not disrupt the existing VDOMs.

For this example, firewalls are only included to deal with web traffic. This is to provide an example without making configuration unnecessarily complicated.

This example includes the following sections:

- Network topology and assumptions
- General configuration steps
- Configuring common items
- Creating virtual domains
- Configuring the Company_A VDOM
- Configuring the Company_B VDOM

- Configuring the VLAN switch and router
- Testing the configuration

Network topology and assumptions

Each organization's internal network consists of a different range of IP addresses:

- 10.11.0.0/255.255.0.0 for Company A.
- 10.12.0.0/255.255.0.0 for Company B.

For the procedures in this section, it is assumed that you have enabled VDOM configuration on your FortiGate. For more information, see VDOMs overview.

The VDOM names are similar to the company names for easy recognition. The root VDOM can't be renamed and is not used in this example.

Interfaces used in this example are port1 and port2. Some FortiGate models may not have interfaces with these names. port1 is an external interface. port2 is an internal interface.

General configuration steps

The following steps summarize the configuration for this example. For best results, follow the procedures in the order given. Also, note that if you perform any additional actions between procedures, your configuration may have different results.

1. Configuring common items
2. Creating virtual domains
3. Configuring the Company_A VDOM
4. Configuring the Company_B VDOM
5. Configuring the VLAN switch and router
6. Testing the configuration

Configuring common items

Both VDOMs require you configure security profiles. These will be configured the same way, but need to be configured in both VDOMs.

The relaxed profile allows users to surf websites they are not allowed to visit during normal business hours. Also a quota is in place to restrict users to one hour of access to these websites to ensure employees don't take long and unproductive lunches.

To create a strict web filtering profile - GUI:

1. Go to the proper VDOM, and select **Security Profiles > Web Filter**.
2. Select **Create New**.
3. Enter `strict` for the **Name**.
4. Expand FortiGuard Web Filtering, and select block for all Categories except Business Oriented, and Other.
5. Block all Classifications except Cached Content, and Image Search.
6. Ensure **FortiGuard Quota** for all Categories and Classifications is Disabled.
7. Select **OK**.

To create a strict web filtering profile - CLI:

```
config vdom
   edit <vdom_name>
      config webfilter profile
         edit strict
            config ftgd-wf
               set allow g07 g08 g21 g22 c01 c03
               set deny g01 g02 g03 g04 g05 g06 c02 c04 c05 c06 c07
            end
            set web-ftgd-err-log enable
         end
```

To create a relaxed web filtering profile - GUI:

1. Go to the proper VDOM, and select **Security Profiles > Web Filter**.
2. Select **Create New**.
3. Enter `relaxed` for the **Name**.
4. Expand FortiGuard Web Filtering, and select block for Potentially Security Violating Category, and Spam URL Classification.
5. Enable FortiGuard Quotas to allow 1 hour for all allowed Categories and Classifications.

Creating virtual domains

The FortiGate supports 10 virtual domains. Root is the default VDOM. It can't be deleted or renamed. The root VDOM is not used in this example. New VDOMs are created for Company A and Company B

To create the virtual domains - GUI:

1. With VDOMs enabled, select **Global > System > VDOM**.
2. Select **Create New**.
3. Enter `Company_A` for Name, and select **OK**.
4. Select **Create New**.
5. Enter `Company_B` for Name, and select **OK**.

To create the virtual domains - CLI:

```
config system vdom
   edit Company_A
   next
   edit Company_B
end
```

Configuring the Company_A VDOM

This section describes how to add VLAN subinterfaces and configure security policies for the Company_A VDOM.

This section includes the following topics:

- Adding VLAN subinterfaces
- Creating the Lunch schedule

- Configuring Company_A firewall addresses
- Creating Company_A security policies

Adding VLAN subinterfaces

You need to create a VLAN subinterface on the port2 interface and another one on the port1 interface, both with the same VLAN ID.

To add VLAN subinterfaces - GUI:

1. Go to **Global > Network > Interfaces**.
2. Select **Create New**.
3. Enter the following information and select **OK**:

Name	VLAN_100_int
Interface	port2
VLAN ID	100
Virtual Domain	Company_A

4. Select **Create New**.
5. Enter the following information and select **OK**:

Name	VLAN_100_ext
Interface	port1
VLAN ID	100
Virtual Domain	Company_A

To add the VLAN subinterfaces - CLI:

```
config system interface
   edit VLAN_100_int
      set interface port2
      set vlanid 100
      set vdom Company_A
   next
   edit VLAN_100_ext
      set interface port1
      set vlanid 100
      set vdom Company_A
   end
```

Creating the Lunch schedule

Both organizations have the same lunch schedule, but only Company A has relaxed its security policy to allow employees more freedom in accessing the Internet during lunch. Lunch schedule will be Monday to Friday from 11:45 AM to 2:00 PM (14:00).

To create a recurring schedule for lunchtime - GUI:

1. In Company_A VDOM, go to **Policy & Objects > Schedules**.
2. Select **Create New**.
3. Enter `Lunch` as the name for the schedule.
4. Select **Mon**, **Tues**, **Wed**, **Thu**, and **Fri**.
5. Set the **Start** time as `11:45` and set the **Stop** time as `14:00`.
6. Select **OK**.

To create a recurring schedule for lunchtime - CLI:

```
config vdom
   edit Company_A
      config firewall schedule recurring
         edit Lunch
            set day monday tuesday wednesday thursday friday
            set start 11:45
            set end 14:00
         end
```

Configuring Company_A firewall addresses

For Company A, its networks are all on the 10.11.0.0 network, so restricting addresses to that domain provides added security.

To configure Company_A firewall addresses - GUI:

1. In the Company_A VDOM, go to **Policy & Objects > Addresses**.
2. Select **Create New**.
3. Enter `CompanyA` in the **Address Name** field.
4. Type 10.11.0.0/255.255.0.0 in the **Subnet / IP Range** field.
5. Select **OK**.

To configure vdomA firewall addresses - CLI:

```
config firewall address
   edit CompanyA
      set type ipmask
      set subnet 10.11.0.0 255.255.0.0
   end
```

Creating Company_A security policies

A security policy can include varying levels of security feature protection. This example only deals with web filtering. The following security policies use the custom security `strict` and `relaxed` profiles configured earlier.

For these security policies, we assume that all protocols will be on their standard ports, such as port 80 for HTTP traffic. If the ports are changed, such as using port 8080 for HTTP traffic, you will have to create custom services for protocols with non-standard ports, and assign them different names.

The firewalls configured in this section are:

- internal to external — always allow all, security features - web filtering: strict
- internal to external — Lunch allow all, security features - web filtering:relaxed

Security policies allow packets to travel between the internal VLAN_100 interface to the external interface subject to the restrictions of the protection profile. Entering the policies in this order means the last one configured is at the top of the policy list, and will be checked first. This is important because the policies are arranged so if one does not apply the next is checked until the end of the list.

To configure Company_A security policies - GUI:

1. Go to **Policy & Objects > IPv4 Policy**.
2. Select **Create New**.
3. Enter the following information and select **OK**:

Name	CompanyA-lunch
Incoming Interface	VLAN_100_int
Outgoing Interface	VLAN_100_ext
Source Address	CompanyA
Destination Address	all
Schedule	Lunch
Service	all
Action	ACCEPT
Security Features	enable
Web Filtering	relaxed

This policy provides relaxed protection during lunch hours — going from strict down to scan for protocol options and web filtering. AntiVirus and Email Filtering remain at strict for security — relaxing them would not provide employees additional access to the Internet and it would make the company vulnerable.

1. Select **Create New**.
2. Enter the following information and select **OK**:

Name	CompanyA-strict
Incoming Interface	VLAN_100_int
Outgoing Interface	VLAN_100_ext
Source Address	CompanyA
Destination Address	all
Schedule	always

Service	all
Action	ACCEPT
Security Features	enable
Web Filtering	strict

This policy enforces strict scanning at all times, while allowing all traffic. It ensures company policies are met for network security.

4. Verify that the policy list arranged **By Sequence** to make sure the CompanyA-lunch policy is located above the CompanyA-strict policy. If necessary, rearrange the policies so that the appropriate policy is applied to outgoing traffic.

To configure Company_A security policies - CLI:

```
config vdom
   edit Company_A
      config firewall policy
         edit 1
            set name "CompanyA-lunch"
            set srcintf VLAN_100_int
            set dstintf VLAN_100_ext
            set srcaddr all
            set dstaddr all
            set action accept
            set schedule Lunch
            set webfiltering relaxed
         next
         edit 2
            set name "CompanyA-strict"
            set srcintf VLAN_100_int
            set dstintf VLAN_100_ext
            set srcaddr all
            set dstaddr all
            set action accept
            set schedule always
            set webfiltering strict
         end
```

Configuring the Company_B VDOM

This section describes how to add VLAN subinterfaces and configure security policies for the Company B VDOM.

This section includes the following topics:

- Adding VLAN subinterfaces
- Creating Company_B service groups
- Configuring Company_B firewall addresses
- Configuring Company_B security policies

Adding VLAN subinterfaces

You need to create a VLAN subinterface on the internal interface and another one on the external interface, both with the same VLAN ID.

To add VLAN subinterfaces - GUI:

1. Go to **Network > Interfaces**.
2. Select **Create New**.
3. Enter the following information and select **OK**:

Name	VLAN_200_int
Interface	port2
VLAN ID	200
Virtual Domain	Company_B

4. Select **Create New**.
5. Enter the following information and select **OK**:

Name	VLAN_200_ext
Interface	port1
VLAN ID	200
Virtual Domain	Company_B

To add the VLAN subinterfaces - CLI:

```
config system interface
   edit VLAN_200_int
      set interface internal
      set vlanid 200
      set vdom Company_B
   next
   edit VLAN_200_ext
      set interface external
      set vlanid 200
      set vdom Company_B
   end
```

Creating Company_B service groups

Company_B does not want its employees to use any online chat software except NetMeeting, which the company uses for net conferencing. To simplify the creation of a security policy for this purpose, you create a service group that contains all of the services you want to restrict. A security policy can manage only one service or one group.

To create a chat service group - GUI:

1. Go to **Policy & Objects > Services** and select **Create New > Service Group**.
2. Enter `Chat` in the **Group Name** field.

3. For each of IRC, AOL, SIP-MSNmessenger and TALK, select the service in the **Available Services** list and select the right arrow to add it to the **Members** list.

If a particular service does not appear in the **Available Services** list, see the list in **Policy & Objects > Services**. Some services don't appear by default unless edited.

4. Select **OK**.

To create a games and chat service group - CLI:

```
config firewall service group
   edit Chat
      set member IRC SIP-MSNmessenger AOL TALK
   end
```

Configuring Company_B firewall addresses

Company B's network is all in the 10.12.0.0 network. Security can be improved by only allowing traffic from IP addresses on that network.

To configure Company_B firewall address - GUI:

1. In the Company_B VDOM, go to **Policy & Objects > Addresses.**
2. Select **Create New**.
3. Enter `new` in the **Address Name** field.
4. Type 10.12.0.0/255.255.0.0 in the **Subnet / IP Range** field.
5. Select **OK**.

To configure Company_B firewall addresses - CLI:

```
config vdom
   edit Company_B
      config firewall address
         edit all
            set type ipmask
            set subnet 10.12.0.0 255.255.0.0
         end
```

Configuring Company_B security policies

Security policies allow packets to travel between the internal and external VLAN_200 interfaces subject to the restrictions of the protection profile.

To configure Company_B security policies - GUI:

1. Go to **Policy & Objects > IPv4 Policy**.
2. Select **Create New**.
3. Enter the following information and select **OK**:

Name	CompanyB-deny-games-chat
Incoming Interface	VLAN_200_int

Outgoing Interface	VLAN_200_ext
Source Address	all
Destination Address	all
Schedule	BusinessDay
Service	games-chat
Action	DENY

This policy prevents the use of network games or chat programs (except NetMeeting) during business hours.

4. Enter the following information and select **OK**:

Name	CompanyB-lunch
Incoming Interface	VLAN_200_int
Outgoing Interface	VLAN_200_ext
Source Address	all
Destination Address	all
Schedule	Lunch
Service	HTTP, DNS
Action	ACCEPT
Security Features	enable
Web Filter	relaxed

This policy relaxes the web category filtering during lunch hour.

5. Select **Create New**.
6. Enter the following information and select **OK**:

Name	CompanyB-strict
Incoming Interface	VLAN_200_int
Outgoing Interface	VLAN_200_ext
Source Address	all
Destination Address	all
Schedule	BusinessDay

Service	HTTP, DNS
Action	ACCEPT
Security Profiles	enabled
Web Filter	strict

This policy provides rather strict web category filtering during business hours.

7. Select **Create New**.
8. Enter the following information and select **OK**:

Name	CompanyB-after-hours
Incoming Interface	VLAN_200_int
Outgoing Interface	VLAN_200_ext
Source Address	all
Destination Address	all
Schedule	always
Service	ANY
Action	ACCEPT
Security Profiles	enabled
Web Filter	relaxed

Because it is last in the list, this policy applies to the times and services not covered in preceding policies. This means that outside of regular business hours, the Relaxed protection profile applies to email and web browsing, and online chat and games are permitted. Company B needs this policy because its employees sometimes work overtime. The other companies in this example maintain fixed hours and don't want any after-hours Internet access.

To configure Company_B security policies - CLI:

```
config firewall policy
   edit 1
      set name "CompanyB-deny-games-chat"
      set srcintf VLAN_200_int
      set srcaddr all
      set dstintf VLAN_200_ext
      set dstaddr all
      set schedule BusinessDay
      set service Games
      set action deny
   next
   edit 2
      set name "CompanyB-lunch"
      set srcintf VLAN_200_int
```

```
        set srcaddr all
        set dstintf VLAN_200_ext
        set dstaddr all
        set action accept
        set schedule Lunch
        set service HTTP
        set profile_status enable
        set profile Relaxed
    next
    edit 3
        set name "CompanyB-strict"
        set srcintf VLAN_200_int
        set srcaddr all
        set dstintf VLAN_200_ext
        set dstaddr all
        set action accept
        set schedule BusinessDay
        set service HTTP
        set profile_status enable
        set profile BusinessOnly
    next
    edit 4
        set name "CompanyB-after-hours"
        set srcintf VLAN_200_int
        set srcaddr all
        set dstintf VLAN_200_ext
        set dstaddr all
        set action accept
        set schedule always
        set service ANY
        set profile_status enable
        set profile Relaxed
    end
```

Configuring the VLAN switch and router

The Cisco switch is the first VLAN device internal passes through, and the Cisco router is the last device before the Internet or ISP.

This section includes the following topics:

- Configuring the Cisco switch
- Configuring the Cisco router

Configuring the Cisco switch

On the Cisco Catalyst 2900 ethernet switch, you need to define the VLANs 100, 200 and 300 in the VLAN database, and then add configuration files to define the VLAN subinterfaces and the 802.1Q trunk interface.

Add this file to Cisco VLAN switch:

```
!
interface FastEthernet0/1
switchport access vlan 100
!
interface FastEthernet0/5
switchport access vlan 300
```

```
!
interface FastEthernet0/6
switchport trunk encapsulation dot1q
switchport mode trunk
!
```

Switch 1 has the following configuration:

Port 0/1	VLAN ID 100
Port 0/3	VLAN ID 200
Port 0/6	802.1Q trunk

Configuring the Cisco router

The configuration for the Cisco router in this example is the same as in the basic example, except we add VLAN_300. Each of the three companies has its own subnet assigned to it.

The IP addressees assigned to each VLAN on the router are the gateway addresses for the VLANs. For example, devices on VLAN_100 would have their gateway set to 10.11.0.1/255.255.0.0.

```
!
interface FastEthernet0/0
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/0.1
 encapsulation dot1Q 100
 ip address 10.11.0.1 255.255.0.0
!
interface FastEthernet0/0.3
 encapsulation dot1Q 200
 ip address 10.12.0.1 255.255.0.0
!
```

The router has the following configuration:

Port 0/0.1	VLAN ID 100
Port 0/0.3	VLAN ID 200
Port 0/0	802.1Q trunk

Testing the configuration

Use diagnostic commands, such as tracert, to test traffic routed through the network.

You should test traffic between the internal VLANs as well as from the internal VLANs to the Internet to ensure connectivity.

For additional troubleshooting, see Troubleshooting VDOMs.

This section includes the following topics:

- Testing traffic from VLAN_100 to the Internet
- Testing traffic from VLAN_100 to VLAN_200

Testing traffic from VLAN_100 to the Internet

In this example, a route is traced from VLANs to a host on the Internet. The route target is www.example.com.

From a host on VLAN_100, access a command prompt and enter this command:

```
C:\>tracert www.example.com
Tracing route to www.example.com [208.77.188.166]
over a maximum of 30 hops:
 1 <10 ms <10 ms <10 ms 10.100.0.1
...
14 172 ms 141 ms 140 ms 208.77.188.166
Trace complete.
```

The number of steps between the first and the last hop, as well as their IP addresses, will vary depending on your location and ISP. However, all successful tracerts to www.example.com will start and end with these lines.

Repeat the tracert for VLAN_200.

The tracert for each VLAN will include the gateway for that VLAN as the first step. Otherwise, the tracert should be the same for each VLAN.

Testing traffic from VLAN_100 to VLAN_200

In this example, a route is traced between two internal networks. The route target is a host on VLAN_200. The Windows traceroute command `tracert` is used.

From VLAN_100, access a Windows command prompt and enter this command:

```
C:\>tracert 10.12.0.2
Tracing route to 10.12.0.2 over a maximum of 30 hops:
1 <10 ms <10 ms <10 ms 10.100.0.1
2 <10 ms <10 ms <10 ms 10.12.0.2
Trace complete.
```

You can repeat this for different routes in the topology. In each case the IP addresses will be the gateway for the starting VLAN, and the end point at the ending VLAN.

Troubleshooting VDOMs

This section addresses common problems and specific concerns that you may encounter when using VDOMs. All steps assume that you are accessing the management VDOM and have access to global and per-VDOM settings.

This section includes:

- The option to enable VDOMs is missing
- Administrators can't access their assigned VDOM
- Your FortiGate is running slowly
- Your license for additional VDOMs doesn't appear
- You can't delete a VDOM
- A non-management VDOM isn't working with SNMP

The option to enable VDOMs is missing

If the option to enable VDOMs doesn't appear in the GUI, connect to the CLI and use the following command:

```
config system global
   set vdom-admin enable
end
```

Administrators can't access their assigned VDOM

Use the following steps to troubleshoot administrator access:

1. Confirm that the administrator is assigned to the correct VDOM by going to **Global > System > Administrators**. Edit the administrator account and make sure **Virtual Domain** is set to the right VDOM.
2. Confirm that the administrator is using the correct FortiGate interface to access the VDOM by going to **Global > Network > Interfaces**. Edit the interface and make sure **Virtual Domain** is set to the right VDOM and **Administrative Access** allows the proper protocols.

If the interface is referenced by the configuration, you can't change which VDOM it's assigned to.

3. If you have a remote administrator, make sure that the administrator is using an interface that is part of the same VDOM as the group the administrator is a part of.

Your FortiGate is running slowly

When using VDOMS, your FortiGate may run slowly because you either have configured too many VDOMs or one or more VDOMS are consuming too many system resources.

If you have configured many VDOMs on your system, the performance of your FortiGate may be affected. Each VDOM you create on your FortiGate requires system resources to function - CPU cycles, memory, and disk space. When there are too many VDOMs configured there are not enough resources for operation.

If you have sufficient hardware to support the number of VDOMs you're running, check the global resources on your FortiGate by going to **Global > System > Global Resources**. If any VDOM uses more resources than desired, you can set limits as appropriate.

Your license for additional VDOMs doesn't appear

When you apply a license for more VDOMs on your FortiGate, it may take up to 4 hours for the license to appear on the FortiGate. To speed this process up, you can run the CLI command `execute update-now` to tell the FortiGate to update all licenses.

You can't delete a VDOM

The root VDOM can't be deleted.

If you aren't able to delete a VDOM, make sure that nothing in the current configuration doesn't reference that VDOM, including interfaces, routes, and policies. To check if there are any current references, go to **Global > System > VDOM** and look at the **Ref.** column. The number of references to each VDOM is listened.

When you select the number, a list of the references opens. You may be able to delete some references directly from this list. Others, such as interface assignment, must be changed using the main GUI page, such as **Network > Interfaces**.

A non-management VDOM isn't working with SNMP

Because SNMP is configured as a global setting, traps can only be sent to interfaces that belong to the management VDOM.